From Syndicates to Protocols: Rethinking Organized Crime in the Age of Cybercrime

Arthur Hartmann*

Hochschule für Öffentliche Verwaltung Bremen – University of Applied Sciences in Public Administration, Bremen, Director of the Jean Monnet Centre of Excellence Crime Investigations and Criminal Justice, Doventorcontrescarpe 172 C, 28195 Bremen, Germany

Abstract: This article develops the concept of cyber-mediated organized crime to capture structural transformations driven by digital infrastructures, especially cryptocurrencies.

Integrating functionalist theory (AGIL), Elias's figurational sociology, and trust theory, it reconstructs how criminal formations adapt by substituting social embeddedness with cryptographic mechanisms.

Empirical domains—ransomware, darknet markets, blockchain laundering—reveal how digital actors fulfill core functions of protection, coordination, and trust under pseudonymity and decentralization.

Rather than replicating traditional hierarchies, these formations emerge as adaptive social systems shaped by functional differentiation and technological affordances.

Their systemic resilience, despite evolving law enforcement strategies, underscores new modes of illicit governance and contestation.

Keywords: Cybercrime, Organized Crime, Figurational Sociology, AGIL Framework, Functional Equivalence, Cybercrime Infrastructures, Cryptocurrencies, NFT (Non Fungible Tokens), Money Laundering.

1. INTRODUCTION – TOWARDS A CONCEPT OF CYBER-MEDIATED ORGANIZED CRIME

The integration of digital infrastructures into organized crime challenges conventional criminological paradigms rooted in hierarchy, territory, and physical violence. Rather than treating cybercrime as a distinct or secondary category, this article introduces the concept of cyber-mediated organized crime to describe how digital environments reshape the conditions, modalities, and systemic functions of criminal cooperation—across a wide spectrum from fully digital operations to traditionally rooted groups adapting to new technological contexts.

Drawing on Di Nicola's (2022) spectrum theory and recent empirical insights into ransomware groups (Whelan *et al*., 2024), we argue that criminal formations can achieve coordination, differentiation, and trust without stable identities or physical proximity. To theorize these dynamics, we mobilize structural functionalism and figurational sociology—demonstrating how classical approaches illuminate emerging forms of cooperation and systemic adaptation.

The article proceeds in five steps: Chapter 2 outlines conceptual foundations and research strategy; Chapter 3 introduces the concepts of functional equivalence and figurational sociology and applies the AGIL framework to cyber-mediated crime; Chapter 4 analyzes empirical cases; and Chapters 5 and 6 discuss theoretical implications and conclusions.

Prevailing conceptions of organized crime and cybercrime significantly influence legislation, jurisprudence, and prosecutorial practice. In Germany, for example, a misguided statutory definition of criminal organizations led to the widespread perception that organized crime was virtually absent—reflecting legal categories rather than empirical realities.

2. MATERIALS AND METHODS

This article employs a theory-driven, interpretive research strategy to investigate how organized crime adapts under digital conditions. Rather than generating primary data, it systematically synthesizes existing empirical studies—on ransomware networks, illicit online markets, blockchain infrastructures, and law enforcement reports (*e.g.*, FBI, BKA)—through the lens of sociological theory.

For practical reasons, only studies and literature in English and German were considered. In line with the journal's orientation, preference was given to openly accessible sources.

Its methodological focus lies in the reconstruction of systemic functions (drawing on Parsons' AGIL schema)

*Address correspondence to this author at the Hochschule für Öffentliche Verwaltung Bremen – University of Applied Sciences in Public Administration, Bremen, Director of the Jean Monnet Centre of Excellence Crime Investigations and Criminal Justice, Doventorcontrescarpe 172 C, 28195 Bremen, Germany; E-mail: arthur.hartmann@hfoev.bremen.de

E-ISSN: 1929-4409/25

and interdependence relations (based on Elias's figurational sociology). This dual framework enables the identification of structural continuities and innovations in cyber-mediated organized crime across a broad spectrum of digital transformation—from fully virtual formations to traditional groups operating in increasingly digitized environments.

Andrea Di Nicola (2022) reconceptualizes organized crime through the notion of "digital organized crime" and introduces a spectrum theory that avoids binary categorizations between traditional and cybercriminal organizations. His model captures the hybridity and fluidity of contemporary formations, shaped by digital infrastructures and dispersed cooperation. He calls for a "digital sociology of organized crime," integrating digital sociology, Science and Technology Studies (STS), and processual criminology to analyze how human actors and technological systems co-produce deviance and control.

However, the conceptual boundaries between 'digital organized crime' and 'cybercrime' remain fluid, and the term 'digital organized crime' may gradually lose its analytical precision as emerging technologies—such as quantum computing—reshape the digital landscape. To address this, we propose the term cyber-mediated organized crime. This term aligns with the European Commission's typology of cybercrime and builds on foundational work by Wall (2005, 2015), McGuire and Dowling (2013), and Cormier and McKenzie (2022). It is designed to capture a broad continuum ranging from cyber-assisted to cyber-dependent offenses, emphasizing that digital infrastructures mediate not only the technical execution of crimes but also the structural transformation of criminal cooperation and systemic embeddedness.

3. RESULTS – FUNCTIONAL SUBSTITUTION AND DIGITAL COOPERATION

This section presents the principal findings of the analysis.

Regarding cybercrime we use Di Nicola's (2022) typology of cyber-dependent, cyber-enabled, and cyber-assisted crime. Across the spectrum, digital infrastructures facilitate secrecy, coordination, and coercion. Even cyber-dependent phenomena like distributed denial-of-service (DDoS) attacks can manifest organizational features akin to those of conventional criminal syndicates. Whelan *et al.* (2024) empirically demonstrate how ransomware groups fulfill structural and functional characteristics of organized crime, as defined by von Lampe (2015). These include systematic criminal activity, durable offender structures, and extra-legal governance.

While cybercrime formations may exhibit the structural and functional traits of organized crime, the ways in which these characteristics are realized differ significantly from conventional syndicates. Ransomware actors, for instance, coordinate through affiliate programs, enforce rules via reputational systems, and maintain specialized roles—approximating traditional organized crime without hierarchical command or physical proximity, as will be illustrated in Chapter 4.

This raises the question of whether cybercrime constitutes a genuinely novel phenomenon or merely represents a classical form of deviance adapted to new technological infrastructures. Observations of technological change tend to emphasize novelty, often giving rise to rhetorics of revolutionary transformation, suggesting that nothing will ever be the same again. Yet we must ask: how different must something be to be recognized as new?

Giuseppe Tomasi di Lampedusa's novel *The Leopard* (2007 [1958]) offers a subtle reflection on this very tension. Set during the Risorgimento—the Italian unification process—the novel portrays the reconfiguration of power in Sicily and the emergence of Mafia. Through the voice of its protagonist, Don Fabrizio, Prince of Salina, the novel suggests that everything may need to change so that, in essence, everything can remain the same. This insight captures the paradoxical interplay of innovation and persistence. Accordingly, the distinction between "new" and "old" should not rely on technological surfaces but on deeper analytical criteria. In sociology and institutional analysis, structural configurations and systemic functions have long served as more robust indicators of social change than visible appearances or toolkits.

3.1. Functional Equivalents

The functional analysis of societal subsystems—institutions, organizations, and individuals—dates back to Auguste Comte (1798–1857), who distinguished between "social statics" (structure) and "social dynamics" (change) as foundational categories of sociological inquiry (Castro, 2009). Originally rooted in biology, this analytical perspective shaped classical sociology from Spencer, Durkheim, and Pareto to

Parsons and Luhmann (Castro, 2009; Görke & Scholl, 2007; Hall, 2001; Husa, 2015; Luhmann, 1987 and 2024; Wenzel, 2001).

At its core lies a key insight: essential system functions—such as nutrition, transport, or social control—can be realized through structurally divergent means. Whether food is secured through hunting or industrial production, or goods are transported by ox cart or airplane, what matters analytically is the fulfillment of systemic functions. This principle of functional equivalence—the substitution of different mechanisms serving the same purpose—has since informed sociology, psychology, political science, and computer science (Hall, 2001; Jitsumori, 2001).

In the realm of organized crime, this concept clarifies how structurally dissimilar formations can serve equivalent systemic roles. In The Sicilian Mafia, Gambetta (1993) conceptualizes organized crime as a market for private protection where trust is scarce and contractual guarantees are absent. This creates a "communication dilemma": criminals must signal credibility and coercive capacity without attracting law enforcement attention (pp. 20–21). Symbolic gestures—religious donations, public rituals—build reputation under opacity (pp. 34–35).

In digital environments, this logic shifts from social ritual to technical infrastructure. As shown in Chapter 4, darknet actors use escrow systems, rating mechanisms, and algorithmic feedback to establish trust—functional equivalents to Gambetta's communicative tactics, adapted to pseudonymity and decentralization.

Functional equivalence also helps resolve long-standing controversies between "organized" and "disorganized" crime (Wall, 2023). According to von Lampe (2015), key features of organized crime include systemic criminal activity, durable offender structures, and extralegal governance. If these functions are fulfilled then decentralized gangs or micro-networks may also qualify. Early studies by Conwell and Sutherland (1937) already emphasized how peripheral activities contribute to cohesion and norm transmission. Von Lampe's (2024) notion of "criminal associations"—spaces of mutual aid and normative regulation—further illustrates how organizational functions can emerg outside formal command structures.

In sum, cyber-mediated crime need not replicate the form of traditional syndicates to be functionally equivalent. If it performs the core tasks of coordination, enforcement, and resource extraction, it qualifies as "organized" in a systemic sense—even when digitally mediated and structurally diffuse.

3.2. Parson's AGIL Scheme

According to von Lampe (2015), organized crime is characterized by systematic criminal activity, durable offender structures, and extralegal governance. While there is little doubt that cybercrime groups engage in systematic illegal conduct, it is less clear whether their pseudonymous and often transient forms of cooperation amount to durable structures in a sociological sense. This ambiguity underscores the need to move beyond surface-level descriptions and assess whether such formations fulfill broader systemic functions—such as identity formation, strategic adaptability, and normative continuity.

Parsons's AGIL framework (1951) provides a powerful tool for this analysis. It conceptualizes the necessary functions any social system must fulfill to persist: Adaptation (A) to external conditions, Goal Attainment (G) through coordinated action, Integration (I) via normative regulation, and Latency (L), which ensures cultural continuity and internal value reproduction (Wenzel, 2001). Though often criticized for abstraction and normative bias (Sciulli, 2001; Tittenbrun, 2013), AGIL remains analytically productive—especially for comparing disparate organizational forms. Bales's (1951) Interaction Process Analysis (IPA) provides empirical grounding for AGIL, validating its focus on socio-emotional cohesion and task orientation in small group dynamics (Wenzel, 2001).

In the context of cybercrime, AGIL helps to illuminate how digital formations maintain coherence without central authority. Adaptation is evident in the use of mixers and anonymizing technologies; Goal Attainment is realized through monetized ransomware operations; Integration is supported by escrow systems and feedback loops; and Latency is maintained through platform norms, pseudonymity, and the continuity of digital personas (Opielka, 2004; Treviño, 2005). These functions demonstrate that even decentralized, pseudonymous groups can satisfy the systemic imperatives that define organized crime.

From this perspective, even loosely affiliated actors—such as ransomware affiliates or darknet vendors—may be considered functionally organized if

they collectively fulfill the AGIL imperatives. Their decentralized structure does not indicate disorganization, but rather a strategic adaptation to enforcement environments. As Kasper and Bulanova-Hristova (2017: 40) note, the dismantling of online platforms rarely leads to the cessation of criminal activity but rather to fragmentation and diversification. This is evident in the reconfiguration of ransomware ecosystems following the takedowns of groups like LockBit and BlackCat (BKA, 2025, 19). Historical parallels reinforce this point: both the Mafia, in the wake of the Maxi Trials or the First Mafia War, and terrorist networks like al-Qaeda or ISIS after major countermeasures, adapted flexibly without collapsing.

The continuity of illicit cooperation across structural ruptures is further illustrated by the adaptability of Hong Kong Triads during the COVID-19 pandemic, as they swiftly exploited emerging opportunities (Luk, 2022). Even the Mafia—often seen as the prototype of rigidly hierarchical organized crime—has displayed considerable structural diversity. While Cressey (1969) described the American La Cosa Nostra as a functionally differentiated bureaucracy, Hess (1998) emphasized dyadic patron–client relationships within the Sicilian Mafia until at least the 1970s. Both models have been widely challenged as empirically problematic (Lupo, 2005). These examples suggest that functional coherence and organizational durability can exist beyond formal hierarchy—whether analog or digital.

3.3. Figurational Sociology

To complement the abstraction and normative bias of Parsons's theory, this section draws on Norbert Elias's figurational sociology. Elias offers a dynamic, process-oriented perspective on society centered on figurations—networks of interdependent individuals whose relationships evolve over time. Rejecting dualisms such as individual vs. society, Elias proposed a relational and historical sociology that links micro-level psychology with macro-level social change (Fan *et al*., 2024), conceptualizing individuals and institutions as co-evolving within webs of interdependence (Elias, 1978).

Elias understood power not as a possession but as a fluctuating balance within interdependent relations. Norms and emotions are likewise shaped by long-term social processes rather than individual volition. In *The Civilizing Process*, Elias (2000) traced how social norms gradually fostered self-restraint, connecting sociogenesis (social change) and psychogenesis (personality formation). His concept of the "king mechanism" shows how early court societies consolidated power through symbolic capital, emotional regulation, and bureaucratic control (Elias, 1983). These developments not only transformed institutions but also raised thresholds of shame and self-regulation (Elias, 2000; Fan *et al*., 2024; van Krieken, 2017; Wouters and Mennell, 2015).

A comparable transformation can be observed in cyber-dependent crime. Traditional hierarchies based on kinship or territory give way to modular cooperation (e.g., Ransomware-as-a-Service), pseudonymity, and platform governance. As shown in Chapter 4, these are not merely technical shifts but reconfigurations of social and emotional structures.

The emotional implications are substantial. The absence of direct victim contact lowers empathic barriers, fostering a pragmatic, emotionally detached offender habitus. Offenders interact via dashboards rather than face-to-face, using code instead of coercion—a shift toward "emotional flattening."

Despite its explanatory potential, figurational sociology remains underused in criminology. Though applied to organizations (van Krieken, 2019) and violence (Malešević & Ryan, 2013), its relevance for understanding digital criminal cooperation is only beginning to emerge. This article suggests that cyber-mediated organized crime entails a figurational transformation—reshaping both coordination and the emotional economies of deviance.

3.4. Summary: Functional Logic and Structural Shifts in Cybercrime

The analysis of cyber-mediated criminal formations through the lenses of functional equivalence, AGIL imperatives, and figurational sociology reveals a consistent pattern: despite their decentralized and pseudonymous character, these structures fulfill the essential systemic functions of organized crime. They adapt to environmental pressures through technical innovations (e.g., mixers, encryption), pursue clear goals (e.g., monetization through ransomware), integrate participants via reputation systems and norms, and reproduce internal values through pseudonym continuity and platform-specific cultures.

What distinguishes these formations from traditional organized crime is not the absence of structure, but its reconfiguration. Hierarchy, territory, and face-to-face loyalty are replaced by modular cooperation, cryptographic governance, and affective detachment.

Platforms such as darknet markets or Ransomware-as-a-Service ecosystems show how algorithmic trust, role specialization, and performance-based incentives enable coordinated illicit action at scale—even without centralized command.

Figurational sociology adds an important emotional dimension. The transition from embodied violence to symbolic and technical enforcement is accompanied by a shift in offender habitus: emotional flattening, instrumental rationality, and detachment from harm. Offenders operate through dashboards and protocols, not through social proximity or kin-based loyalty.

These insights challenge binary distinctions between "organized" and "disorganized" crime. As shown in the following chapter, even fragmented cybercrime groups can act as functionally coherent systems—reproducing trust, enforcing norms, and resisting state control. Recognizing these shifts is essential for both criminological theory and effective policy-making.

4. EMPIRICAL MANIFESTATIONS OF THEORETICAL CONCEPTS IN CYBER-DEPENDENT ORGANIZED CRIME

This chapter demonstrates how the theoretical lenses developed above—functional equivalence, the AGIL schema, and figuration—manifest in cyber-dependent organized crime. We focus on cryptographic infrastructures and digital platforms as key enablers of coordination, trust-building, and systemic resilience.

As traditional control mechanisms such as physical proximity and territorial dominance lose relevance, digital criminal ecosystems increasingly rely on pseudonymity, modular cooperation, and automated enforcement. These features are particularly evident in ransomware-as-a-service operations, cryptocurrency mixers, and darknet markets.

Drawing on recent empirical findings, we show how cryptographic technologies restructure not only the organization of crime but also its emotional dynamics and public perception. Sociological theory helps to illuminate how trust, power, and coordination emerge under digital conditions—without replicating the hierarchies of traditional organized crime.

4.1. Cryptocurrencies as Infrastructures of Trust, Obfuscation, and Systemic Substitution

Cryptocurrencies such as Bitcoin and Ethereum have become indispensable to cyber-dependent organized crime, as their decentralized structure aligns with the fluid, modular architecture of contemporary criminal formations (Di Nicola, 2020; Groysman, 2023; Hamilton & Leuprecht, 2024; Wall, 2023). As Katagiri (2022) notes, actors transitioned from prepaid cards to cryptocurrencies. Today, cryptocurrencies are not merely targets of theft and extortion but constitute core infrastructures for payment, laundering, and asset protection across illicit domains including ransomware, darknet trade, investment fraud, and money laundering (Kasper & Bulanova-Hristova, 2017: 37–39; Lapuh Bele, 2021; Reddy & Minnaar, 2018). Paired with anonymizing tools such as Tor, mixers, and privacy coins, they form a resilient ecosystem of pseudonymous financial exchange.

While blockchains guarantee transparency and immutability, obfuscation mechanisms shield real-world identities (Gjorgjev *et al.*, 2025; Passas, 2025). Mixers like Helix, Bitcoin Fog, and Blender.io dissolve transaction chains (Groysman, 2023), while stealth addresses and privacy coins enable trust without social embeddedness—replacing interpersonal assurances with cryptographic enforcement (Blue, 2025). Bitcoin mining itself has been used for laundering: sanctioned individuals and states, including North Korea, convert electricity into untainted cryptocurrency (Weisser & Bliesener, 2025).

Non-fungible tokens (NFTs) extend this logic to digital goods. Their symbolic legitimacy, combined with pseudonymous trading and lack of market benchmarks, facilitates value obfuscation. Through wash trading and artificial pricing, illicit funds are laundered via seemingly unique digital assets (Weisser & Bliesener, 2024).

From a functionalist perspective, these technologies fulfill multiple AGIL imperatives: Goal Attainment via performance incentives and monetization; Integration through escrow, rating, and algorithmic safeguards; Latency via pseudonymity and platform norms; and Adaptation through laundering strategies that bypass traditional financial intermediaries (Lapuh Bele, 2021). Wallets like Wasabi and Samurai illustrate how pseudonymity becomes structurally embedded in illicit exchange.

These technologies operate as functional equivalents to traditional mechanisms of loyalty, secrecy, and protection—without relying on kinship or face-to-face accountability. As Lustig and Nardi (2015) and Walton and Dhillon (2017) argue, blockchain-based trust is algorithmic: legitimacy emerges from protocol compliance rather than interpersonal bonds.

An instructive analogue is the Hawala system—an informal value transfer mechanism rooted in trust, reputation, and social sanction (Jost & Sandhu, 2016; Passas, 2006; Soudjin, 2015). Like blockchain infrastructures, Hawala facilitates Integration without institutional oversight, operating through networked interdependence and norm enforcement.

This transformation also reconfigures criminal figurations. As Elias (2000) emphasized, shifts in interdependence reshape both organizational structure and emotional orientation.

The prototypical figure of traditional organized crime is the uomo d'onore of the Sicilian Mafia—an individual whose sociocultural habitus is defined by loyalty, secrecy, and masculine honor. This identity is sustained by the code of omertà, a vow of silence that fosters internal solidarity while rejecting any cooperation with external authorities (Dondoni *et al*., 2006). Initiation rituals, often imbued with Catholic symbolism, sacralize organizational membership and instill a quasi-religious allegiance to the group (Merlino, 2012). Within this moral universe, violence becomes a regulated means of asserting dominance, preserving internal order, and safeguarding collective prestige (Mondello *et al*., 2019). While this ethos draws on traditional Sicilian values—familism, patriarchal authority—it is reconfigured into a codified subculture that legitimizes violence and criminality in the name of honor and social stability.

Yet this habitus also conceals the brutality and greed of its members. It obscures the Mafia's rigid hierarchies, its territorial domination by so-called families—which do not necessarily consist of kinship ties but govern clearly demarcated and enduring regions—and the cyclical struggles for power, influence, and betrayal within the organization (Lupo, 2005: 25). This structure characterizes both the so-called "old" Mafia and the "new" Mafias of past and present (Lupo, 2005: 31).

In contrast, cybercrime replaces bodily presence and ritualized loyalty with dashboards, ratings, and pseudonymous credibility. Trust and status are no longer anchored in face-to-face relationships but encoded in reputation scores and access hierarchies. Nevertheless, affect persists: cybercriminal communities like Dark0de regulate participation through peer recognition, ironic banter, and exclusion—mirroring older forms of symbolic boundary-setting and internal discipline (Sawicka *et al*., 2023).

Importantly, cryptocurrencies have extended beyond cyber-dependent offenses and now underpin a broad spectrum of criminal economies. Digital currencies are central to drug distribution (Tzanetakis & South, 2023: 103) and have been adopted by traditional criminal groups adapting to cyber-mediated infrastructures. As the FBI (2024: 9) notes, this includes ransomware, identity theft, fraud, and business email compromise—demonstrating how digital tools have become integral to both emerging and established illicit operations. What links these diverse formations is the shared objective of acquiring financial capital and social status—inside and outside the criminal field.

This shift illustrates systemic adaptation. As state surveillance and enforcement intensify, criminal actors increasingly rely on cryptographic disintermediation and anonymizing technologies (Whelan, 2024). Tropina (2012) observes that cybercriminal operations increasingly resemble corporate structures, developing sophisticated criminal-to-criminal (C2C) business models.

In sum, digital infrastructures do not dissolve social relations—they reencode them. Cryptocurrencies replace personal trust with cryptographic assurance, enabling illicit cooperation without physical proximity. Rather than signaling the decline of organized crime, this transformation reflects its ongoing structural and emotional reconfiguration in the digital age.

4.2. Platform-Driven Trust and Distributed Criminal Economies

Darknet marketplaces such as AlphaBay, Hydra, and Dream Market emulate legitimate e-commerce platforms by offering product listings, vendor ratings, customer reviews, and escrow services (Décary-Hétu & Giommoni, 2017; Di Nicola, 2020; Europol, 2022; Tzanetakis, 2018). These features establish algorithmic trust systems, where credibility is earned through persistent pseudonyms, verifiable delivery, and positive feedback—addressing Gambetta's dilemma of signaling reliability under conditions of anonymity (Andrei *et al.*, 2025).

To prevent fraud, platforms enforce formal rules and deploy escrow systems that release payments only after contractual obligations are met. Vendor identities are verified through PGP encryption and long-standing key fingerprints, enabling continuity even across shifting pseudonyms. Trust, formerly embedded in

personal ties, becomes protocol-based, with legitimacy derived from algorithmic governance (Kasper & Bulanova-Hristova, 2017: 31–34; Lustig & Nardi, 2015).

Tropina (2012) highlights the flexible and horizontal nature of such formations: "the power of the group is in the strength and sophistication of its software, not in the number of individuals" (p. 53). This infrastructure reproduces trust while also performing key AGIL functions. Goal Attainment arises from incentive structures and dispute resolution, while Integration is achieved through feedback systems and internal governance—functional equivalents to traditional social mechanisms.

Yet anonymity does not eliminate emotional dynamics. In collectives like Dark0de, platforms cultivate affective regimes—ironic banter, peer recognition, and exclusion rituals—which sustain cooperation and informal norm enforcement (Sawicka *et al.*, 2023). Elias's figuration theory helps explain how even pseudonymous interactions become emotionally structured within emergent webs of interdependence.

The shift from face-to-face contact to cryptographic mediation thus represents a broader figural transformation: organized crime becomes decentralized, scalable, emotionally flattened, yet normatively encoded. Darknet markets exemplify how technological architectures substitute both the social and affective foundations of trust in traditional criminal organizations.

4.3. The Rise of Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service (RaaS) illustrates how digital infrastructures transform criminal cooperation. In this model, malware developers maintain codebases while affiliates—recruited via darknet forums—select targets, launch attacks, and negotiate ransoms. Payments are executed in cryptocurrency, and revenues distributed via automated or manual wallet-splitting. This modular labor division enables scalable collaboration without centralized authority (Katagiri, 2024; Whelan *et al.*, 2024). As Blue (2025) notes, such interactions are anonymous, transactional, and minimally interpersonal—yet enable labor division, specialization, and monetization (Kasper & Bulanova-Hristova, 2017: 20–22).

These ecosystems resemble the gig economy (Di Nicola, 2020): tasks are fragmented, relationships ephemeral, and roles filled by pseudonymous freelancers. Risk exposure is differentiated; actors choose roles based on risk-reward calculations, complicating attribution and deterrence (Hamilton & Leuprecht, 2023). RaaS exemplifies this structure: developers provide malware, affiliates execute attacks, and ransoms are paid in cryptocurrency (Lapuh Bele, 2021). According to Katagiri (2022), this model succeeded by integrating reliable crypto-based payment mechanisms that adapted to enforcement pressures.

The operational scale is significant. In 2024, the FBI (2024, 9) recorded 3,159 ransomware complaints in the U.S. Germany reported 950 severe cases in 2024 (BKA 2025: 17). Bitkom estimated cyberattack-related damages at €178.6 billion in 2024—€30.4 billion more than in 2023—accounting for 75% of total reported economic harm (BKA 2025: 2). Global ransom payments averaged over $450,000; total transactions exceeded $800 million in 2024, down from $1.25 billion in 2023 (BKA 2025: 20). Preventive corporate measures have reduced data encryption but increased extortion via data exposure (BKA 2025: 21).

RaaS is not rooted in kinship or territory but in functional interdependence. Roles are interchangeable, incentives performance-based, and reputation maintained through escrow, feedback, and referral systems (Whelan *et al.*, 2024; Tzanetakis & South, 2023: 106). These arrangements fulfill AGIL imperatives: adaptation (resilience under enforcement), goal attainment (profit-driven collaboration), integration (technical trust mechanisms), and latency (platform norms and pseudonymous persistence).

From an Eliasian perspective, RaaS reflects a post-relational figuration: cooperation is disembedded, emotionally flattened, and automated. Affiliates operate with minimal affective ties. Violence is outsourced to code; trust is programmable; moral distance from victims is maximized—especially in attacks on hospitals or schools.

Unlike Gambetta's model of private protection, RaaS imposes coercion unilaterally. There is no implicit contract or reciprocal expectation. This marks a rupture from traditional extortion, where relational embeddedness played a regulatory role.

The pivotal role of cryptocurrency becomes clearer when contrasted with older product extortion cases like the 1982 Tylenol poisonings. Historically, such offenses rarely succeeded due to payment logistics: bank transfers were traceable, and physical handovers exposed offenders. Nearly half of extortionists

abandoned attempts after a single anonymous contact; only a very small minority completed payment and escaped undetected; estimated at less than 1% (Moschesus, 2004: 78–82).

RaaS changed this logic. By leveraging anonymous payments—especially Bitcoin—criminals reduce exposure and enable scalable, low-risk extortion. These same infrastructures are now accessible to traditional offenders. Cryptographic payment systems may therefore revive classic extortion strategies once hindered by logistical constraints.

4.4. Visibility, Adaptation, and State Response

Cyber-mediated organized crime introduces novel structural and emotional configurations, yet it remains vulnerable to state intervention. High-profile operations—EncroChat, Sky ECC, ANOM, and most recently the 2023 Hive takedown—demonstrate law enforcement's increasing capacity to penetrate encrypted infrastructures. The German Federal Criminal Police Office (BKA, 2025: 27–28) reports successful takedowns of Crimemarket, Nemesis Market, AegisTools, and major malware loaders (*e.g.*, IcedID, Bumblebee, Trickbot) as part of Operation Endgame. Operation Final Exchange resulted in the seizure of 47 crypto exchanges and over 140 servers suspected of laundering illicit assets and violating AML norms.

This evolving confrontation illustrates a dynamic counter-figuration: state agencies increasingly deploy cryptographic infiltration, metadata analysis, and predictive modeling. Yet, the intensification of surveillance prompts offenders to deepen their reliance on cryptographic disintermediation—circumventing conventional oversight (Groysman, 2023; Walton & Dhillon, 2017; Whelan *et al.*, 2024). Platform shutdowns often prove short-lived: the closure of Silk Road was quickly followed by more robust successors, demonstrating the black market's systemic resilience (Kasper & Bulanova-Hristova, 2017: 40).

These developments reflect Elias's theory of interdependent power balances: the adaptive interplay between illicit innovation and institutional response. Publicized takedowns reframe crime as both elusive and governable—shaping societal discourses on privacy, transparency, and state authority (Dondjio, 2023; Passas, 2025). Despite technical advances, the systemic embeddedness of cyber-mediated crime suggests it is unlikely to be eradicated. As a functionally adaptive social system, it will continue to evolve its technical, economic, and normative operations in response to investigative pressure—sustaining its AGIL imperatives under shifting conditions.

4.5. Platform Hierarchies and the Figuration of Digital Illegality

While much of the literature emphasizes the decentralized nature of online illicit platforms, Kasper and Bulanova-Hristova (2017) offer a contrasting interpretation. Based on income disparities and differentiated access to platform functions, they identify a stratified structure in carding forums and cryptomarkets, consisting of five roles: administrators, moderators, reviewers, reviewed vendors, and regular users. This stratification recalls Cressey's (1969, 113-115) mafia pyramid, with a clear top-down hierarchy.

Yet such models risk conflating functional differentiation with command hierarchy. As critics of mafia myths have long argued (Ianni & Reuss-Ianni, 1972; Chambliss, 1978; Block, 1980; Haller, 1990), differences in status or income do not equate to institutional authority in a Weberian sense. Online platforms lack coercive mechanisms: exclusion or reputational damage—rather than violence—remain the principal sanctions (Kasper & Bulanova-Hristova, 2017: 26; Lusthaus, 2012: 89).

From a systems-theoretical perspective, these platforms represent functionally differentiated structures rather than hierarchies. Roles evolve to meet AGIL imperatives: innovation (adaptation), moderation (integration), norm enforcement (latency), and monetization (goal attainment). Authority is contingent, reversible, and often rooted in technical skill or symbolic capital rather than formal command (Wall, 2023).

Elias's figuration theory helps elucidate these dynamics: power is not a fixed resource but emerges from shifting interdependencies. Cyber-mediated criminal formations are fluid and decentralized, governed not by command structures but by symbolic capital—trust, irony, exclusion. Their structural regularities reflect evolving relational configurations rather than institutionalized hierarchies.

This marks a key distinction from classical organized crime, which aligns more closely with Max Weber's (1972: 541) concept of *legitimate domination* (*Herrschaft*): a stable framework of command and obedience, legitimized by tradition, charisma, or

rational-legal authority (Orsini, 2024: 157). In contrast, digital formations are stratified but not hierarchical: they involve unequal roles—some actors hold more influence, reputation, or access—but lack a centralized authority with the power to issue binding commands.

Elias's concept of figuration is especially useful here, as it emphasizes that power arises from relational dependencies and fluctuates with them. While Weber captures the rule-bound structure of formal hierarchy, Elias provides a lens for analyzing decentralized, emergent orders in which domination is negotiated, contingent, and historically embedded (Dondoni *et al*., 2006).

Importantly, the absence of formal hierarchy and physical coercion differentiates these configurations from traditional criminal milieus. Disputes are typically resolved through reputational or technical means—such as DDoS attacks, defamation, or exclusion—rather than lethal violence. These mechanisms serve functionally equivalent purposes but differ fundamentally from the sanctioned killings that characterized intra-organizational conflict in classical contexts, such as during the First Mafia War in 1962 (Lupo, 2005: 286).

5. DISCUSSION – RETHINKING ORGANIZATION, RESILIENCE, AND THE ROLE OF THE STATE

This chapter reflects on the broader theoretical and policy implications of the preceding analysis. It examines how digital infrastructures reconfigure criminal cooperation, enabling new forms of organization, emotional regulation, and systemic resilience. Drawing on the concept of counter-figuration, it also considers evolving state responses, the contested visibility of cybercrime, and the normative challenges posed by cryptographic technologies. The findings suggest that cyber-mediated organized crime is not a chaotic field of opportunism, but a functionally integrated and adaptively resilient formation.

The article set out to develop a sociologically grounded framework for conceptualizing cyber-mediated organized crime. In response to Di Nicola's (2022) call for a digital sociology of deviance, we explored how criminal cooperation persists and adapts under digital conditions—without simply replicating conventional organizational forms.

Structural functionalism, operationalized via Parsons's AGIL schema, proved analytically productive. Decentralized formations—such as ransomware ecosystems or blockchain-based infrastructures—fulfill key systemic functions (adaptation, goal attainment, integration, latency) through pseudonymity, automation, and protocol-based governance. These functional equivalents challenge typologies centered on hierarchy, territory, or violence.

Elias's process sociology added depth by situating these configurations within shifting emotional regimes and interdependencies. Cyber-mediated crime reflects broader transformations in trust, risk, and resistance to state control. Importantly, technological mediation does not imply a linear "civilizing" process: ransomware attacks on hospitals and the strategic use of crypto-mining by sanctioned regimes illustrate the persistence of harm and conflict.

Rather than proposing wholly new theories, we advocate a conceptual extension of classical sociology. Functionalist and figurational approaches remain well suited to analyzing the systemic and emotional logic of cyber-mediated deviance. A contemporary criminology of cybercrime must be both technologically literate and sociologically anchored.

The practical relevance of this framework becomes clear at the level of legislation, which should not rely on outdated models of classical or cyber-mediated organized crime that rarely align with empirical realities. This disconnect is mirrored in judicial interpretation and law enforcement practice. For instance, German courts have consistently refused to adapt to the EU Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime in their interpretation of Section 129 of the German Criminal Code, which addresses "criminal associations."

The Framework Decision, based on the UN Convention against Transnational Organized Crime (UN Palermo Convention), adopts a broad definition of criminal organization and structured association (Article 1), explicitly encompassing networked formations. Developed through expert consultations involving academics, journalists, law enforcement, and civil society, it reflects contemporary insights into organized crime.

By contrast, German jurisprudence has traditionally interpreted Section 129 narrowly—resulting in a significant underrepresentation of organized crime in official statistics. In 2021, for example, only eight individuals were convicted under this provision. This sustains the perception that organized crime poses little threat in Germany. Even recent amendments and

case law have not fully overcome these limitations (Hartmann, 2022; 2025 forthcoming).

Consequently, police investigations often fail to align with prosecutorial requirements and inadequately capture relevant phenomena. This mismatch continues to shape public perceptions, underestimating the scope and systemic embeddedness of organized crime in its digital forms.

6. CONCLUSION: FROM DIGITAL TOOLS TO CRIMINAL FIGURATIONS

Cyber-mediated organized crime is not a transient deviation but a structurally embedded mode of illicit cooperation. This article has demonstrated how digital infrastructures foster new forms of trust, specialization, and coordination—substituting physical control with cryptographic protocols and rigid hierarchies with flexible, role-based configurations. Drawing on Parsons's AGIL model and Elias's figuration theory, we argue that these formations are not disorganized anomalies but functionally and emotionally adapted to the digital environment.

For criminological research, this opens the path toward theoretically grounded frameworks that can distinguish fluid but systemically embedded criminal formations from spontaneous collaborations among offenders. While the latter may act adaptively and purposefully, they are not embedded in durable social systems and thus do not fulfill the latency function essential to organized crime.

As state responses become more sophisticated, they encounter adversaries that are equally adaptive. Law enforcement increasingly relies on data analytics, infiltration, and international cooperation—yet offenders respond with cryptographic disintermediation, decentralization, and modular cooperation. This dynamic interplay underscores the need for criminological approaches that move beyond typologies of groups and offenses to examine systemic relations between technological innovation, institutional reaction, and illicit transformation.

Future research should deepen the integration between sociological theory and empirical inquiry—particularly through digital ethnography, network analysis, and the study of platform-mediated trust systems. The growing role of artificial intelligence in both crime commission and surveillance invites critical engagement with emerging technologies and their governance. In parallel, legal frameworks must be reexamined in light of functionally equivalent, yet structurally novel forms of deviance that defy traditional categories of command, territory, or violence.

A sociology of organized crime must therefore remain attuned to both continuity and change: to the enduring dynamics of illicit cooperation, and to the historically novel infrastructures under which they now unfold.

FUNDING

This article was written within the framework of the Jean Monnet Centre of Excellence for Crime Investigations and Criminal Justice. However, the author received no specific funding or support for this work.

RESEARCH ETHICS AND POLICIES

This research is based exclusively on the analysis of publicly available sources and secondary literature.

CONFLICT OF INTEREST

The article was written within the framework of the Jean Monnet Centre of Excellence Crime Investigations and Criminal Justice, but no specific funding was received for this article.

ACKNOWLEDGEMENTS

The article is single-authored.

CONSENT FOR PUBLICATION

The manuscript does not include any identifiable individual data, images, or audio-visual material requiring consent.

REFERENCES

Andrei, Filippo and Giuseppe Alessandro Veltri. 2025. "Signalling Strategies and Opportunistic Behaviour: Insights from Dark-net Markets." *PLoS ONE* 20(3):e0319794. https://doi.org/10.1371/journal.pone.0319794

Bales, Robert F. 1951. *Interaction Process Analysis: A Method for the Study of Small Groups*. 2nd ed. Cambridge, MA: Addison-Wesley Press. (Originally published 1950.) Retrieved July 2025 (https://dn790006.ca.archive.org/0/items/interactionproce00bale/interactionproce00bale.pdf).

Bancroft, Angus. 2020. „Managing trust relationships in digital crime." *Journal of Criminology and Digital Society* 6(2):135–152.

Block, Alan A. 1980. *East Side – West Side – Organizing Crime in New York 1930 – 1950*. Cardiff: University College Cardiff Press.

Blue, Lisa E. 2025. "Cryptocurrencies are here to stay! Think you aren't vulnerable, think again." *International Journal of Criminology and Sociology* 14:56–67. https://doi.org/10.6000/1929-4409.2025.14.6

Bundeskriminalamt (BKA; Federal Criminal Police Office). 2025. *Bundeslagebild Cybercrime 2024*. Wiesbaden: Bundeskriminalamt.

Castro, José Esteban. 2009. "Functionalism (including Structural Functionalism)". Pp. 277–282 in *International Encyclopedia of Human Geography,* edited by R. Kitchin and N. Thrift. London: Elsevier.

Chamblis, William, J. 1978. *On the Take – From Petty Crooks to Presidents*. Bloomington: Indiana University Press.

Conwell, Clara, and Edwin H. Sutherland. 1937. *The Professional Thief: By a Professional Thief.* Annotated and interpreted by E. H. Sutherland. Chicago, IL: University of Chicago Press.

Cormier, Marc, and Sarah McKenzie. 2022. "Cyber-Dependent and Cyber-Enabled Crime: Legal Responses and Challenges." Pp. 99–128 in *Legal Issues in Information Technology* edited by M. Perry, A. Roy, M. de Zwart, M. Adams, N. Selvadurai, H. Forrest, M. Cormier, and S. McKenzie. Toronto: Thomson Reuters.

Council of the European Union. 2008. *Council Framework Decision 2008/841/JHA of 24 October 2008 on Combating Organised Crime*. Official Journal of the European Union L 300:42–45. Retrieved July 2, 2025 (https://eur-lex.europa.eu/eli/dec_framw/2008/841/oj/eng).

Cressey, Donald R. 1969. *Theft of the Nation: The Structure and Operations of Organized Crime in America*. New York, NY: Harper & Row. (Reprinted 2008, Piscataway, NJ: Transaction Publishers)

Di Lampedusa, Giuseppe Tomasi. 2007. *The Leopard*. Translated by Archibald Colquhoun. London: Vintage Books (Originally published 1958 as Il Gattopardo; first English edition 1960 by Collins, UK). ISBN 186046145X.

Di Nicola, Andrea. 2022. "Towards digital organized crime and digital sociology of organized crime." *Trends in Organized Crime*. Published online May 30, 2022. https://doi.org/10.1007/s12117-022-09457-y

Dondjio, Cyrille Y. 2023. "Navigating Ethical Challenges in Cryptocurrency and Blockchain Technologies." *International Journal of Technoethics* 14(1), 1–15. https://doi.org/10.4018/IJT.328091

Décary-Hétu, David, & Luca, Giommoni. 2017. "Do Police Crackdowns Disrupt Drug Cryptomarkets? A Longitudinal Analysis of the Effects of Operation Onymous." *Crime, Law and Social Change* 67(1):55–75. https://doi.org/10.1007/s10611-016-9644-4

Dondoni, Monica, Giuseppe Licari, Elena Faccio, and Anita Pellicciotta. 2006. "Identità e Normatività Gruppali nella Cultura Siciliana e nella Sub-Cultura di Cosa Nostra." *Narrare i Gruppi* 1(1):1–23. Retrieved July 2025 (http://www.narrareigruppi.it/volumi/2006/marzo/dondoni-def.pdf).

Elias, Norbert. 1978. *What Is Sociology?* Translated by G. Morrissey and S. Mennell. New York, NY: Columbia University Press. (Originally published 1970 as *Was ist Soziologie?*).

Elias, Norbert. 1983. *The Court Society*. Oxford, UK: Blackwell. (Originally published 1969 as *Die höfische Gesellschaft*).

Elias, Norbert 2000. *The Civilizing Process: Sociogenetic and Psychogenetic Investigations*. Oxford, UK: Blackwell. (Originally published 1939 as *Über den Prozess der Zivilisation*).

Elias, Norbert. 2021. "Über die Einsamkeit der Sterbenden in unseren Tagen." Pp. 9–68 in *Gesammelte Schriften*, Vol. 6, edited by H. Hammer. Frankfurt am Main: Suhrkamp. (Originally written 1982; edited on behalf of the Norbert Elias Foundation by R. Blomert, H. Hammer, J. Heilbronn, A. Treibel, and N. Wilterdink.)

European Commission. 2023. *Cybercrime*. Retrieved June 2025 (https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en)

Europol. 2021. *OTF Greenlight/Trojan Shield*. Retrieved June 2025 (https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication).

Fan, Ximing, Jason Hughes, Matt McIntosh, and Katherine Hughes. 2024. "Elias, Norbert (1897–1990)." In *The Wiley-Blackwell Encyclopedia of Sociology*, edited by G. Ritzer, C. Rojek, M. J. Ryan. Hoboken, NJ: Wiley. https://doi.org/10.1002/9781405165518.wbeose029.pub2

FBI, Internet Crime Complaint Center. 2024. *Internet Crime Report 2024*. Washington, DC: Federal Bureau of Investigation. Retrieved June 2025 (https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf).

Gambetta, Diego. 1993. *The Sicilian Mafia: The Business of Private Protection*. Cambridge, MA: Harvard University Press.

Görke, Alexander, and Armin Scholl. 2006. "Niklas Luhmann's Theory of Social Systems and Journalism Research." *Journalism Studies* 7(4):644–655. https://doi.org/10.1080/14616700600758066

Gjorgjev, Jelena, Fajar M. F. Ramadhan, and Sonny Dhamayana. 2025. "Blockchain forensics – Unmasking anonymity in dark web transactions." *International Journal of Criminology and Sociology* 14:68–75. https://doi.org/10.6000/1929-4409.2025.14.07

Grabosky, Peter. 2007. "The Internet, Technology, and Organized Crime." *Asian Journal of Criminology* 2(2):145–161. https://doi.org/10.1007/s11417-007-9034-z

Groysman, Igor. 2018. *Revolution in Crime: How Cryptocurrencies Have Changed the Criminal Landscape*. PhD dissertation, John Jay College of Criminal Justice, City University of New York. Retrieved June 2025 (https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1088&context=jj_etds).

Hall, Geoffrey. 2001. "Mechanisms of functional equivalence." European Journal of Behavior Analysis, 2(1):69-71. https://doi.org/10.1080/15021149.2001.11434176

Haller, Mark H. 1990. "Illegal Enterprise: A Theoretical and Historical Interpretation. *Criminology*, 28(2), 207–236. https://doi.org/10.1111/j.1745-9125.1990.tb01324.x

Hamilton, Rhianna & Christian Leuprecht. 2024. The Crime-Crypto Nexus: Nuancing Risk Across Crypto-Crime Transactions. Pp 15-42 in *Financial Crime and the Law. Ius Gentium: Comparative Perspectives on Law and Justice* Vol. 115, edited by D. Goldbarsht, and L. de Koker. Cham, Switzerland: Springer. Retrieved June 2025. https://doi.org/10.1007/978-3-031-59543-1_2

Hartmann, Arthur. 2022. Sec. 129 German Criminal Code "Forming criminal organisations". Pp. 867 – 881 in *Gesamtes Strafrecht. StGB, StPO, Nebengesetze. Legal commentary*, edited by D. Dölling, G. Duttge, S. König, D. Rössner, 5th edition, Baden-Baden: Nomos; 6th edition forthcoming 2025.

Hess, Henner. 1998. *Mafia and Mafiosi: Origin, Power, and Myth*. New York, NY: NYU Press. (Originally published 1970: *Mafia*).

Husa, Jaakko. 2015. "Funktionalism." In *The Encyclopedia of Political Thought* edited by M. T. Gibbons. Hoboken, NJ: Wiley. https://doi.org/10.1002/9781118474396.wbept0398

Ianni, Francis A. and Elizabeth Reuss-Ianni. 1972. *A Family Business. Kinship and Social Control in Organized Crime*. New York: Russell Sage Foundation.

Jitsumori, Masako. 2001. "Emergence of Functional Equivalence." *European Journal of Behavior Analysis* 2(1):75–78. https://doi.org/10.1080/15021149.2001.11434178

Jost, Patrick M. and Harjit Singh. 2016. *The Hawala Alternative Remittance System and its Role in Money Laundering*. Paper prepared by the Financial Crimes Enforcement Network in cooperation with INTERPOL/FOPAC. Retrieved June 2025 (https://web.archive.org/web/20161228041941/https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/FinCEN-Hawala-rpt.pdf).

Kasper, Karsten, and Gergana Bulanova-Hristova. 2017. *Criminal Structures on Illegal Online Platforms: Literature Review Report*. EMPACT – OAP Cyber-Attacks, OA 8.1 "Cybercrime and Organised Crime / Organised Cybercrime." Wiesbaden: Bundeskriminalamt.

Katagiri, Nori. 2024. "From prepaid cards to bitcoin: How did ransomware hackers adopt cryptocurrencies?" *Journal of Cyber Policy*. 9(2):239–255. https://doi.org/10.1080/23738871.2024.2435956

Lapuh Bele, Julija. 2021. "Cryptocurrencies as facilitators of cybercrime". *SHS Web of Conferences*, Vol. 111: 01005. https://doi.org/10.1051/shsconf/202111101005

Luhmann, Niklas. 1987. *Soziale Systeme: Grundriß einer allgemeinen Theorie*. Frankfurt am Main: Suhrkamp.

Luhmann, Niklas. 2024. *Einführung in die Systemtheorie*. Edited by Dirk Baecker. 9th ed. Heidelberg: Carl-Auer Verlag.

Luk, Bryan Tzu Wei. 2023. "When Crime Meets Pandemic: Organized Crimes and Triad Societies' Activities during COVID-19 Pandemic Hong Kong." *Asian Journal of Criminology* 18(2):123–141. https://doi.org/10.1007/s11417-023-09300-4

Lupo, Salvatore. 2005. *Die Geschichte der Mafia*. Düsseldorf: Patmos Verlag. (Originally published 1996 as *Storia della Mafia*).

Lusthaus, Jonathan. 2012. "Trust in the world of cybercrime." *Global Crime* 13(2):71–94. https://doi.org/10.1080/17440572.2012.674183

Lustig, Caitlin, & Bonnie Nardi. 2015. "Algorithmic authority: The case of Bitcoin." Pp. 743–752 In M. J. Ackerman, *et al.* (Eds.), *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS)*. Kauai, HI: IEEE Computer Society. Extended version available as Lustig (2022). https://doi.org/10.48550/arXiv.2201.05939

Malešević, Siniša, & Kevin Ryan. 2013. "The Disfigured Ontology of Figurational Sociology: Norbert Elias and the Question of Violence." *Critical Sociology* 39(2):301–318. https://doi.org/10.1177/0896920511434484

McGuire, Mike & Samantha Dowling. 2013. "Cyber crime: A review of the evidence." *Home Office Research Report 75*. Retrieved June 2025 https://assets.publishing.service.gov.uk/media/5a74fc06e5274a59fa716800/horr75-summary.pdf)

Merlino, Rosella. 2012. "From a Man to a 'Man of Honour': The Role of Religion in the Initiation Ritual of the Sicilian Mafia." *The International Journal of the Humanities,* Annual Review 9(11):59–70. https://doi.org/10.18848/1447-9508/CGP/V09I11/42676

Mondello, Cristina, Luigi Cardia, Elvira Ventura Spagnolo. 2019. "Killing methods in Sicilian Mafia families." *Medico-Legal Journal* 87(1):27–32. https://doi.org/10.1177/0025817218823675

Moseschus, Alexander Marcus. 2004. *Produkterpressung – ein Kriminalphänomen unter kriminologischer, straf- und haftungsrechtlicher sowie taktischer Betrachtungsweise*. Göttingen: Cuvillier Verlag.

Nastri, Michele. 2025. "A Look at the New Developments in the European Union's Regulation on Crypto-Assets and Anti-Money Laundering." *International Journal of Criminology and Sociology* 14: 48–55. https://doi.org/10.6000/1929-4409.2025.14.05

Opielka, Michael. 2019. „Gesellschaftliche Gemeinschaft bei Talcott Parsons und Hegel." Pp. 101–119 in *Handbuch Kommunitarismus* edited by W. Reese-Schäfer. Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-16864-3_5-1

Opielka, Michael. 2004. *Gemeinschaft in Gesellschaft. Soziologie nach Hegel und Parsons*. 2nd edition. Wiesbaden: VS Verlag für Sozialwissenschaften.

Orsini, Alessandro. 2024. *Sociological Theory. From Comte to Postcolonialism*. Cham, Switzerland: Palgrave Macmillan. https://doi.org/10.1007/978-3-031-52539-1_6

Parsons, Talcott. 1951. *The Social System*. New York: Free Press.

Parti, Katalin & Thomas Dearden. 2024. "Cybercrime and Strain Theory: An Examination of Online Crime and Gender." *International Journal of Criminology and Sociology*. Vol. 13, 211–226.

Passas, Nikos. 2025. "Cryptocurrencies, Blockchain, and Financial Crimes." *International Journal of Criminology and Sociology* 14:76–89.

Passas, Nikos & Fabio Coppola. 2025. "Assessing the Effectiveness of Compliance Programs Through the Use of the Metaverse and Blockchain." *International Journal of Criminology and Sociology* 14:90–105.

Passas, Nikos. 2006. "Demystifying Hawala: A Look into its Social Organization and Mechanics." *Journal of Scandinavian Studies in Criminology and Crime Prevention.* 7(1):46–62. https://doi.org/10.1080/14043850601029083

Reddy, Eveshnie and Anthony Minnaa. 2018. "Cryptocurrency: A Tool & Target for Cybercrime." *Acta Criminologica: Southern African Journal of Criminology*, Special Edition: *Cybercrime*, 31(3):71–92.

Sadok, Hicham and Mahammed El Hadi El Maknouzi. 2025. "Can Crypto Currencies Challenge Sovereign Currencies? A Multidisciplinary Overview of Opportunities and Risks." *International Journal of Criminology and Sociology* 14:37–47.

Sawicka, Maia, Angus Bancroft, and Irene Rafanell. 2023. "The emotional infrastructure of a cybercrime collective: Evidence from Dark0de." *Criminology & Criminal Justice (CCJ)*. Article first published online: November 18, 2023. https://doi.org/10.1177/17488958231212412

Sciulli, David. 2001. "Parsons, Talcott (1902–79)." Pp. 11063–11068 in *International Encyclopedia of the Social & Behavioral Sciences* edited by N. J. Smelser and P. B. Baltes. Amsterdam, New York: Elsevier.

Soudjin, Melvin. 2015. "Hawala and Money Laundering: Potential Use of Red Flags for Persons Offering Hawala Services." *European Journal on Criminal Policy and Research* 21(2):191–206. https://doi.org/10.1007/S10610-014-9238-6

Tittenbrun, Jacek. 2013. "Talcott Parsons' economic sociology." *International Letters of Social and Humanistic Sciences* (ILSHS), Vol. 13:20–40. https://doi.org/10.18052/www.scipress.com/ILSHS.13.20

Treviño, A. Javier. 2005. "Parsons's action-system requisite model and Weber's elective affinity: A convergence of convenience." *Journal of Classical Sociology*, 5(3), 303–326. https://doi.org/10.1177/1468795X05057870

Tropina, Tatiana. 2013. "Organized Crime in Cyberspace." Pp. 47–60 in Karriere? Grundschulleitung± edited by W. Bobeth-Neumann. Bielefeld: Transcript Verlag. https://doi.org/10.1515/transcript.9783839424957

United Nations. 2000. *United Nations Convention against Transnational Organized Crime and the Protocols Thereto*. Adopted by the General Assembly on November 15, 2000, by resolution 55/25. Retrieved July 2025 (https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf).

Van Krieken, Robert. 2017. "Norbert Elias and Figurational Sociology". Vol. 4, pp. 1–3 in *The Wiley-Blackwell Encyclopedia of Social Theory*, edited by B. S. Turner, C. Kyung-Sup, C. F. Epstein, P. Kivisto, J. M. Ryan, W. Outhwaite, Hoboken, NJ: Wiley. https://doi.org/10.1002/9781118430873.est0266

Van Krieken, Robert. 2019. "Towards process-figurational theory in organization studies." *Cambio. Rivista sulle trasformazioni sociali* 8(16):141–157. https://doi.org/10.13128/CAMBIO-23911

Wall, David, S. 2005. "The Internet as a Conduit for Criminals." Pp. 77–98 in *Information Technology and the Criminal Justice*

System edited by A.I Pattavina. Thousand Oaks, CA: Sage Publications.

Wall, David, S. 2015. "Dis-organized crime: Towards a distributed model of the organization of cybercrime." *European Review of Organised Crime* 2(2):71–90.

Walton, Joseph, B. and Gurpreet Dhillon. 2017. "Understanding Digital Crime, Trust and Control in Blockchain-Based Systems." *23rd Americas Conference on Information Systems (AMCIS 2017)*. Proceedings Vol. 3, 2351–2360. Boston.

Weisser, N.-F. and C. Bliesener. 2024. „Geldwäsche im digitalen Zeitalter – Non-Fungible Token (NFT)." *Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt)*, pp. 41–47.

Weisser, N.-F. and C. Bliesener. 2025. "Geldwäsche und Terrorismusfinanzierung im digitalen Zeitalter: Umgehung von Sanktionen mit Hilfe des Bitcoin-Mining." *Zeitschrift für Wirtschafts- und Steuerstrafrecht (wistra)*, pp. 133–141.

Wenzel, Harald. 2001. "Functionalism in Sociology". Pp. 5847–5852 in *International Encyclopedia of the Social & Behavioral Sciences* edited by N. J. Smelser and P. B. Baltes. Oxford: Elsevier. https://doi.org/10.1016/B0-08-043076-7/01886-6

Whelan, Chad, David Bright, and James Martin. 2024. "Reconceptualising organised (cyber)crime: The case of ransomware." *Journal of Criminology* 57(1):45–61. https://doi.org/10.1177/26338076231199793

Wouters, Cas and Stephen Mennell. 2015. "Discussing theories and processes of civilisation and informalisation: criteriology." *Human Figurations: Long-term Perspectives on the Human Condition* 4(3):1–25. Retrieved June 2025 (https://norbert-elias.com/wp-content/uploads/2023/11/HF_vol4-n3-2.pdf).

Received on 11-05-2025 Accepted on 05-06-2025 Published on 10-07-2025

https://doi.org/10.6000/1929-4409.2025.14.11